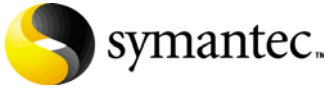
Symantec ESM Integrated Command Engine (ICE) Module Training Guide

For Windows and UNIX



ICE Module Training Guide

The software that is described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 3.0

Copyright Notice

Copyright © 2002 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, Symantec Enterprise Security Manager, LiveUpdate, and Symantec Security Response are trademarks of Symantec Corporation.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other product names that are mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

Technical support

As part of Symantec Security Response, the Symantec Global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features that are available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.htm, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC CORPORATION SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR THE COMPANY OR LEGAL ENTITY THAT WILL BE UTILIZING PRODUCT AND THAT YOU REPRESENT AS AN EMPLOYEE OR AUTHORIZED AGENT ("YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "I DO AGREE" OR "YES" BUTTON OR LOADING THE PRODUCT, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON AND DO NOT USE THE SOFTWARE.

1. LICENSE TO USE

Licensor grants You a non-exclusive, non-transferable license (the "License") for the use of the number of licenses of Licensor's software in machine readable form, and accompanying documentation (the "Product"), on Your machines for which You have been granted a license key and for which You pay the License fee and applicable tax. The License governs any releases, revisions or enhancements to the Product that Licensor may furnish to You.

2. RESTRICTIONS

Product is copyrighted and contains proprietary information and trade secrets belonging to Licensor and/or its licensors. Title to Product and all copies thereof is retained by Licensor nd/or its licensors. You will not use Product for any purpose other than for Your own internal business purposes or make copies of the software, other than a single copy of the software in machine-readable format for back-up or archival purposes. You may make copies of the associated documentation for Your internal use only. You shall ensure that all proprietary rights notices on Product are reproduced and applied to any copies. You may not modify, decompile, disassemble, decrypt, extract, or otherwise reverse engineer Product, or create derivative works based upon all or part of Product. You may not transfer, lease, assign, make available for timesharing or sublicense Product, in whole or in part. No right, title or interest to any trademarks, service marks or trade names of Licensor or its licensors is granted by this License.

3. LIMITED WARRANTY

Licensor will replace, at no charge, defective media and product materials that are returned within 30 days of shipment. Licensor warrants, for a period of 30 days from the shipment date, that Product will perform in substantial compliance with the written materials accompanying the Product on that hardware and operating system software for which it was designed, as stated in the documentation. Use of Product with hardware and/or operating system software other than that for which it was designed and voids this applicable warranty. If, within 30 days of shipment, You report to Licensor that Product is not performing as described above, and Licensor is unable to correct it within 30 days of the date You report it, You may return Product, and Licensor will refund the License fee. If You promptly notify Licensor of an infringement claim based on an existing U.S. patent, copyright, trademark or trade secret, Licensor will indemnify You and hold You harmless against such claim, and shall control any defense or settlement. This warranty is null and void if You have modified Product, combined the Product with any software or portion thereof owned by any third party that is not specifically authorized or failed promptly to install any version of Product provided to You that is non-infringing. If commercially reasonable, Licensor will either obtain the right for You to use the Product or will modify Product to make it non-infringing. The remedies above are Your exclusive remedies for Licensor's breach of any warranty contained herein.

4. LIMITATION OF REMEDIES

THE WARRANTIES IN THIS AGREEMENT ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OF ANY PRODUCT OR ITS DOCUMENTATION. THE LIABILITY OF LICENSOR HEREUNDER FROM ANY CAUSE OF ACTION WHATSOEVER WILL NOT EXCEED THE AGGREGATE LICENSE FEE PAID BY LICENSEE FOR THE PRODUCT. IN NO EVENT WILL LICENSOR OR ITS AUTHORIZED REPRESENTATIVES BE LIABLE FOR LOST PROFITS OR SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF, OR INABILITY TO USE, THE PRODUCT OR LOSS OF OR DAMAGE TO DATA, EVEN IF LICENSOR OR ITS AUTHORIZED REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. LICENSOR AND ITS AUTHORIZED REPRESENTATIVES WILL NOT BE LIABLE FOR ANY SUCH CLAIMS BY ANY OTHER PARTY. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. No action or claim arising out of or relating to this Agreement may be brought by You more than one (1) year after the cause of action is first discovered.

5. CONFIDENTIALITY

You agree that Product and all information relating to the Product is confidential property of the Licensor ("Proprietary Information"). You will not use or disclose any Proprietary Information except to the extent You can document that any such Proprietary Information is in the public domain and generally available for use and disclosure by the general public without any charge or license. Use by persons to which You have contracted any of Your data processing services is permitted only if each contractor (and its associated employees) is subject to a valid written agreement prohibiting the reproduction or disclosure to third parties of software products and associated documentation to which they have access and such prohibitions apply to the Product. You recognize and agree that there is no adequate remedy at law for a breach of this Section, that such a breach would irreparably harm the Licensor and that the Licensor is entitled to equitable relief (including, without limitation, injunctive relief) with respect to any such breach or potential breach, in addition to any other remedies available at law.

6. EXPORT REGULATION

You agree to comply strictly with all US export control laws, including the US Export Administration Act and its associated regulations and acknowledge Your responsibility to obtain licenses to export, re-export or import Product. Export or re-export of Product to Cuba, North Korea, Iran, Iraq, Libya, Syria or Sudan is prohibited.

7. US GOVERNMENT RESTRICTED RIGHTS

If You are licensing Product or its accompanying documentation on behalf of the US Government, it is classified as "Commercial Computer Product" and "Commercial Computer Documentation" developed at private expense, contains confidential information and trade secrets of Licensor and its licensors, and is subject to "Restricted Rights" as that term is defined in the Federal Acquisition Regulations ("FARs"). Contractor/Manufacturer is: Symantec Corporation, and its subsidiaries, Cupertino, California, USA.

8. MISCELLANEOUS

This License is made under the laws of the State of California, USA, excluding the choice of law and conflict of law provisions. Product is shipped FOB origin. This License is the entire License between You and Licensor relating to Product and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communication between the parties during the term of this License. Notwithstanding the foregoing, some Products or products of Licensor may require Licensee to agree to additional terms through Licensor's on-line "click-wrap" license, and such terms shall supplement this Agreement. If any provision of this License is held invalid, all other provisions shall remain valid unless such validity would frustrate the purpose of this License, and this License shall be enforced to the full extent allowable under applicable law. Except for additional terms that may be required through Licensor's on-line "click-wrap" license, no modification to this License is binding, unless in writing and signed by a duly authorized representative of each party. The License granted hereunder shall terminate upon Your breach of any term herein and You shall cease use of and destroy all copies of Product. Duties of confidentiality, indemnification and the limitation of liability shall survive termination or expiration of this Agreement. Any Product purchased by You after the purchase of Product which is the subject of this License shall be subject to all of the terms of this License. All of Symantec Corporation's and its subsidiaries' licensors are direct and intended third-party beneficiaries of this License and may enforce it against You. Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). Licensee may obtain Content Updates for any period for which Licensee has purchased Upgrade Insurance for the Software, entered into a maintenance agreement with Symantec that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates.

Contents

Technical support 3
Licensing and registration 3
Contacting Technical Support 4
Customer Service 4

Symantec ESM ICE module training guide

Introducing the ICE training guide 2
Training prerequisites 2
ICE module components 3
Netstat exercise 4
Running netstat and reviewing its output 5
Building the netstat ICE template 7
Running the ICE module and netstat.ice template 12
Additional netstat exercises 13
NTODrv exercise 14
Running NTODrv and reviewing its output 15
Building the modem ICE template 16
Running the ICE module and modem.ice template 20
Additional NTODrv exercises 21
PSLogList exercise 22
Running PSLogList and reviewing its output 23
Building the eventlog ICE template 24
Running the ICE module and eventlog.ice template 28
Additional PSLogList exercise 29

Symantec ESM ICE module training guide

This guide includes the following topics:

- Introducing the ICE training guide
- Netstat exercise
- NTODrv exercise
- PSLogList exercise

Introducing the ICE training guide

The Integrated Command Engine (ICE) module changes Symantec's Enterprise Security Manager (Symantec ESM) into a dynamic security assessment tool that lets you to identify and implement new checks of your own design.

This guide introduces you to ICE module components and walks you through training exercises using three command line administration utilities: Netstat, NTODrv, and PSLogList.

Training prerequisites

To successfully execute all the training exercises described in this guide, you need the following:

- Microsoft Windows NT, Windows 2000, or Windows XP with Symantec ESM 5.1 or later installed.
- Symantec ESM 5.1 or later installed on Symantec ESM managers and agents in Windows or UNIX domains.
- Current security updates installed on Symantec ESM agents in Windows and UNIX domains.
- Scripts subdirectory under the ESM installation directory (usually /esm on UNIX systems or c:\Program Files\Symantec\ESM on Windows) on at least one of the Symantec ESM manager/agent systems that will be used for the training exercises. Create the Scripts subdirectory and copy Netstat, NTODrv, and PSLogList to the directory.

Note: Netstat is a standard utility available on most Windows and UNIX systems. Download the PSLogList utility from http://www.sysinternals.com. Download the NTODrv utility from: http://www.windowsecurity.com/pages/article.asp?id=454.

ICE module components

The ICE module is delivered with Symantec ESM Security Update releases for Symantec ESM-supported Window and UNIX operating systems.

The ICE module is included in the Symantec ESM default Dynamic Assessment policy. It is installed with the following components:

Table 1-1 ICE module components

Operating system	Component	Description
Windows	\ESM\bin\<architecture>\ice.exe	Main executable
	\ESM\register\<architecture>\ice_t.m	Windows NT .m file with module messages
	\ESM\register\<architecture>\ice_k.m	Windows 2000 .m file with module messages
	\ESM\register\<architecture>\ice_x.m	Windows XP .m file with module messages
UNIX	/esm/bin/<architecture>/ice	Main executable
	/esm/register/<architecture>/ice_u.m	UNIX .m file with module messages

Netstat exercise

This exercise shows you how to integrate the netstat command into the ICE module. In this exercise you will:

- Run the netstat system command on a Windows NT, Windows 2000, Windows XP, or UNIX system and review the output.
- Define the netstat data that you want to capture in an ICE template.
- Run the ICE module to capture and report netstat data.
- Complete related training exercises to test what you have learned.

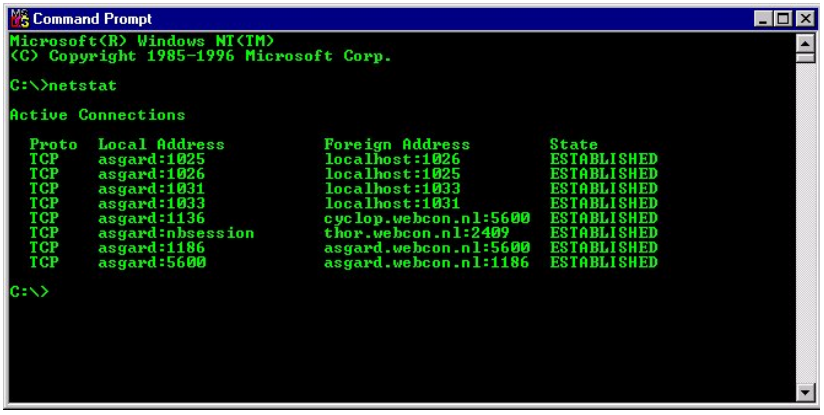
Running netstat and reviewing its output

Netstat is a TCP/IP executable program that queries protocol statistics and current TCP/IP network connections. It is important to monitor these network connections because potential hackers can use ill-configured protocols to break into your systems. Netstat is a standard utility that is available on most Windows and UNIX systems.

To run netstat and review its output

1. If it does not already exist, create the Scripts subdirectory in the ESM directory (usually /esm on UNIX systems or c:\Program Files\Symantec\ESM on Windows) on at least one of the Symantec ESM manager/agent systems that will be used for this training exercise.
2. Copy netstat to the Scripts directory.
3. Run netstat from the Command Prompt and observe the output, which should look like this:

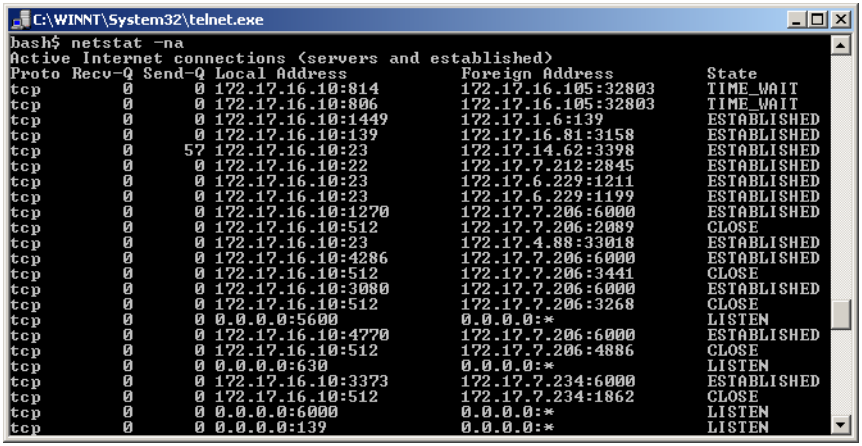
Figure 1-1 Windows netstat output



When you look at the output of the Windows netstat command you can see three distinct fields:

- Introduction: "Active Connections"
- Title line: "Proto," “Local Address,” “Foreign Address,” and “State"
- Data fields: “TCP,” “asgard:1025,” “localhost:1026,” and “ESTABLISHED"

Figure 1-2 UNIX netstat output



This UNIX example is similar:

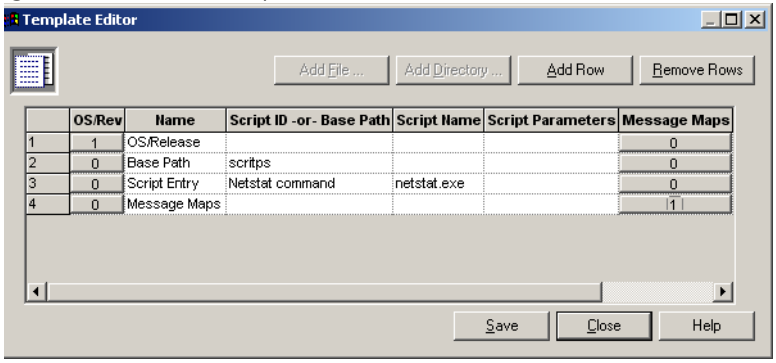
- Introduction: “Internet connections (servers and established)”
- Title line: “Proto,” “Recv-Q,” “Send-Q,” “Local Address,” “Foreign Address,” and “State.”
- Data fields: “tcp,” “0,” “57,” “172.17.16.10:23,” “172.17.14.62:3398,” and “ESTABLISHED.”

Data fields are output for all sockets. You can capture this output in the ICE module by defining a message map in the ICE template.

Building the netstat ICE template

The ICE template determines which command or script is to be run, where that command resides, and what the ICE module should do with the output of the command. In this exercise, you will use the Template Editor to create four template records: OS/Release, Base Path, Script Entry, and Message Maps. At the end of this exercise, your ICE template should look like Figure 1-3.

Figure 1-3 Ice template for Netstat exercise



To create an ICE template based on netstat

To create an ICE template based on netstat, first create a new ICE template and then create the following four template records:

- OS/Release
- Base Path
- Script Entry
- Message Maps

To create an ICE template

1. In the Symantec ESM console tree, right-click **Templates** and select **New**.
2. Select **Integrated Command Engine - all** from the list of available template types.
3. Name the new template **netstat**.

   Note: Do not name the template with a .ice file extension. Symantec ESM automatically adds the .ice extension.

4. Click **OK** and Symantec ESM automatically launches the Template Editor.

To add the OS/Release record to your netstat ICE template

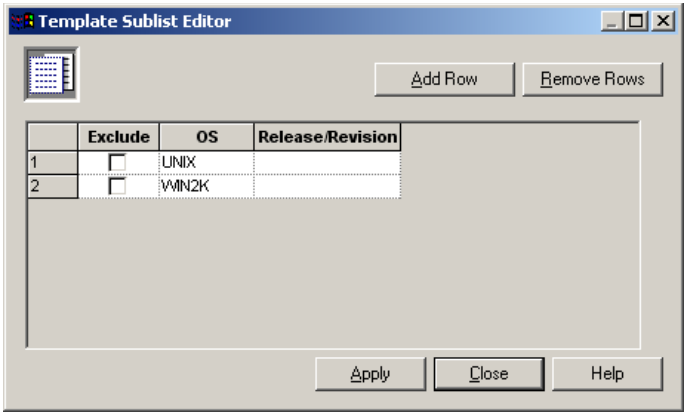
1. In the Template Editor, click **Add Row** to create a new template record.
2. Click the cell under the Name column to access the Name drop-down list and select **OS/Release**.
3. Delete all <NEW> entries from fields.
4. Click the **OS/Rev** button to launch the OS/Rev Sublist Editor. The button displays the number of entries in the OS/Rev sublist. Initially the number is set to 0.
5. In the OS/Rev Sublist Editor, click **Add Row** to add a new sublist record.
6. Click the cell under the OS column to access the OS drop-down list and select the operating system where you want to run the netstat command.

Note: To run the command on both Windows and UNIX agents, select one of the Windows options from the context menu for the first new record, then click **Add Row** and select one of the UNIX options for the second new record.

---

7. Uncheck the Exclude check box.
8. Delete the <NEW> entry in the Release/Revision column.
9. Click **Apply** and then **Close** to return to the Template Editor.

Figure 1-4 Windows and UNIX OS/Rev sublist records



To add the Base Path record to your netstat ICE template

1. In the Template Editor, click **Add Row**.
2. Select **Base Path** from the Name drop-down list.
3. Remove all <NEW> entries from fields.
4. Type **scripts** in the Script ID -or- Base Path column on the Base Path template record. See row 2 in Figure 1-3.

   The Base Path tells the ICE module where the command program is located within the ESM directory. Using installation defaults, **scripts** points to \Program Files\Symantec\Esm\Scripts on Windows systems and to /esm/scripts on UNIX systems.

To add the Script Entry record to your netstat ICE template

1. In the Template Editor, click **Add Row**.
2. Select **Script Entry** from the Name drop-down list.
3. Delete all <NEW> entries from fields.
4. Type **Netstat command** in the Script ID -or- Base Path column of the Script Entry template record.
5. Enter **netstat.exe** for Windows systems or **netstat** for UNIX systems in the Script Name column of the Script Entry template record. This is the name of the program that the ICE module will execute. For Windows, your entries will match row 3 in Figure 1-3 on page 7.

Note: Although several parameters can be used to fine tune the output of the netstat command, no Script Parameters will be defined in this exercise.

To add the Message Maps record to your netstat ICE template

1. In the Template Editor, click **Add Row**.
2. Select **Message Maps** from the Name drop-down list.
3. Delete all <NEW> entries from fields.
4. Click the **Message Maps** button to launch the Message Maps Sublist Editor. The button displays the number of entries in the OS/Rev sublist. Initially the number is set to 0.

Note: You must define at least one message map so the ICE module will know what to do with the output of the netstat command. You can map the command output to any of the following ICE module messages with distinctive names and message classes.

Table 1-2 ICE module messages

Message name	Message title	Class	Security level	Intended to report
Failed	Test failed	1	Yellow	Failed command output
Passed	User test passed	0	Green	Successful command execution
Informational	User test information	0	Green	Information output by a command
Not Applicable	User test not applicable	0	Green	Agent system where command is not relevant
Not Available	User test not available	0	Green	Agent system where command is not accessible
User #1/0 User #2/0 User #3/0	User defined #<> w/value of 0	0	Green	User-customized, class 0 messages
User #1/1 User #2/1 User #3/1	User defined #<> w/value of 1	1	Yellow	User-customized, class 1 messages
User #1/2 User #2/2 User #3/2	User defined #<> w/value of 2	2	Yellow	User-customized, class 2 messages
User #1/3 User #2/3 User #3/3	User defined #<> w/value of 3	3	Yellow	User-customized, class 3 messages

Table 1-2 ICE module messages

Message name	Message title	Class	Security level	Intended to report
User #1/4 User #2/4 User #3/4	User defined #<> w/value of 4	4	Red	User-customized, class 4 messages

Note: You can change these message names and titles so that they are more meaningful to your particular use. For more information on changing messages, see the *Symantec Enterprise Security Manager Security Update User's Guide* for Windows or UNIX.

5 In the Message Maps Sublist Editor, click **Add Row**.

6 Click the cell under the Message column and select **User #1/0** from the drop-down list. This is a green level, user-customized message.

Note: Because the netstat data is not directly related to security, it should be mapped to a green level (or class 0) ICE module message.

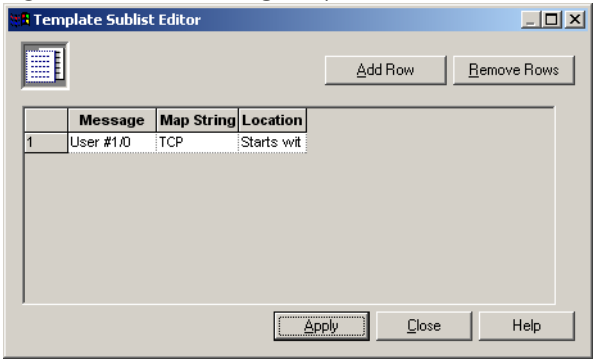
7 In the Map String field, replace the <NEW> entry by typing **TCP** for Windows and **tcp** for UNIX.

Note: Message Maps sublist entries are case sensitive.

8 Click the cell under the Location column and select **Starts with** from the drop-down list. This instructs the ICE module to capture all netstat data that starts with TCP.

Your message map sublist record should look like Figure 1-5.

Figure 1-5 Message map sublist record



9 Click **Apply** and **Close** to close the Template Sublist Editor.

10 Click **Save** and **Close** to save your netstat.ice template.

Running the ICE module and netstat.ice template

You can now run the ICE module to execute netstat and capture its output, using the netstat.ice template that you have created.

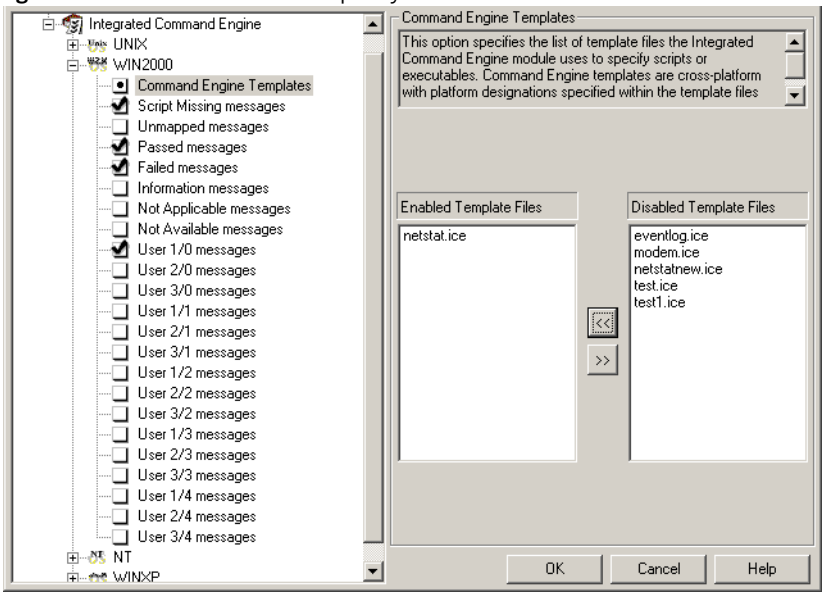
To run the ICE module and capture netstat output

1 Create a new Symantec ESM demonstration policy and add the ICE module to it. For information about creating and using policies, see your *Symantec ESM User Manual*.

2 Open the new policy and enable your netstat.ice template by selecting the **Command Engine Templates** option and moving the netstat.ice template to the Enabled Template Files name list.

3 Verify that the messages that you expect the ICE module to produce are enabled in the ICE module before clicking **OK** to close your demonstration policy.

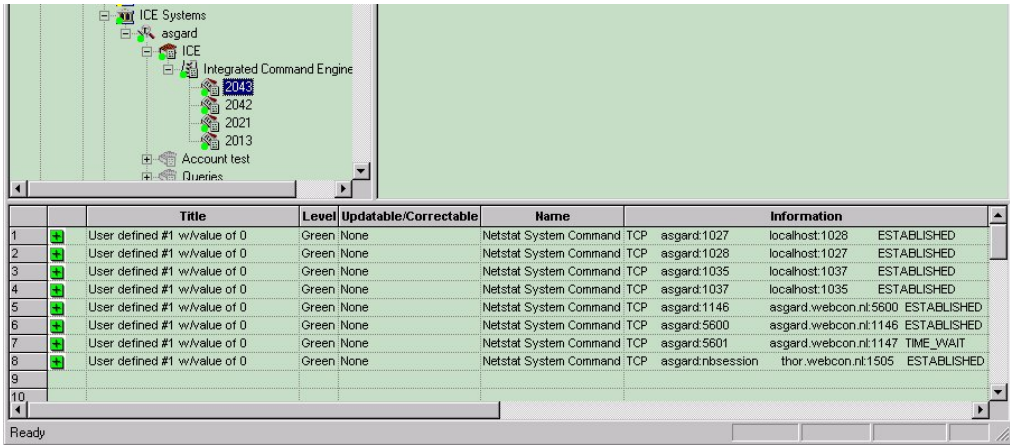
Figure 1-6 Netstat check policy



4 Run the demonstration policy on agents with operating systems that are included by the OS/Release definitions in the netstat.ice template.

The policy run should not take more than a few minutes, depending on the speed of the system and the latency in the network. When the run is completed, the output should look something like Figure 1-7.

Figure 1-7 Captured netstat messages


ICE Systems
asgard
ICE
Integrated Command Engine
2043
2042
2021
2013
Account test
Queries
Title
Level
Updatable/Correctable
Name
Information
1 User defined #1 w/value of 0 Green None Netstat System Command TCP asgard:1027 localhost:1028 ESTABLISHED
2 User defined #1 w/value of 0 Green None Netstat System Command TCP asgard:1028 localhost:1027 ESTABLISHED
3 User defined #1 w/value of 0 Green None Netstat System Command TCP asgard:1035 localhost:1037 ESTABLISHED
4 User defined #1 w/value of 0 Green None Netstat System Command TCP asgard:1037 localhost:1035 ESTABLISHED
5 User defined #1 w/value of 0 Green None Netstat System Command TCP asgard:1146 asgard.webcon.nl:5600 ESTABLISHED
6 User defined #1 w/value of 0 Green None Netstat System Command TCP asgard:5600 asgard.webcon.nl:1146 ESTABLISHED
7 User defined #1 w/value of 0 Green None Netstat System Command TCP asgard:5601 asgard.webcon.nl:1147 TIME_WAIT
8 User defined #1 w/value of 0 Green None Netstat System Command TCP asgard:nbsession thor.webcon.nl:1505 ESTABLISHED
9
10
Ready

Additional netstat exercises

Test what you have learned in the preceding sections of this guide by completing the following additional exercises.

Exercise 1

Enhance the netstat.ice template to also include UDP messages.

Exercise 2

Change the security levels of the TCP messages to Yellow and the UDP messages to Red.

Exercise 3

Look at the netstat output that is illustrated in Figure 1-1 on page 5 and note the socket connections to the local host. Now enhance the netstat.ice template to report only the socket connections to the local host.

NTODrv exercise

This exercise shows you how to integrate the ntodrv command into the ICE module. In this exercise you will:

- Run the NTODrv program on a Windows NT or Windows 2000 system and review the output.
- Define the NTODrv output that you want to capture in an ICE template.
- Run the ICE module to capture and report NTODrv output.
- Complete related training exercises to test what you have learned.

Running NTODrv and reviewing its output

NTODrv is an NT network driver/service query tool that lets you identify the modems that are installed on a Windows NT or Windows 2000 server.

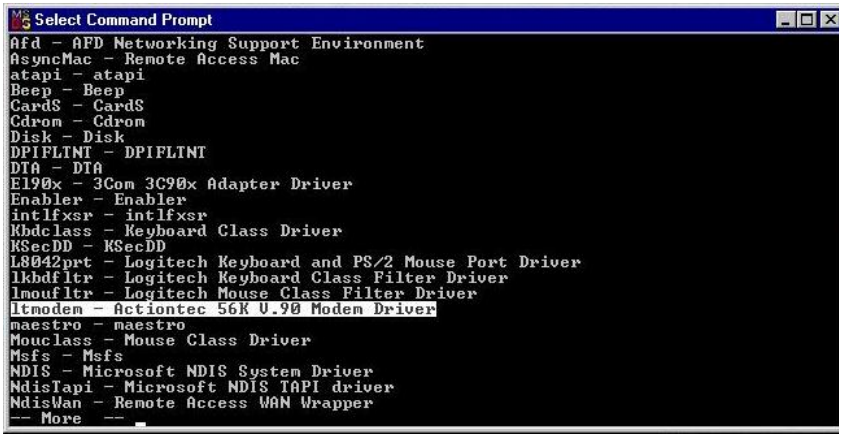
The discovery of existing modems in the enterprise environment is important to security because potential hackers could use these devices to break into the network.

Download the NTODrv utility from:
http://www.windowsecurity.com/pages/article.asp?id=454

To run NTODrv and review its output

1. If it doesn't already exist, create the Scripts subdirectory in the ESM directory (usually c:\Program Files\Symantec\ESM on Windows) on at least one of the Symantec ESM manager/agent systems that will be used for this training exercise.
2. Copy ntodrv to the Scripts directory.
3. Run ntodrv and watch the output, which should look like this:

Figure 1-8 NTODrv output

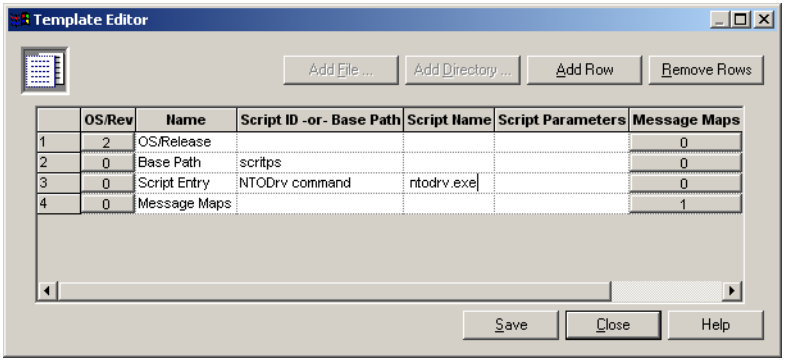

Select Command Prompt
Afd - AFD Networking Support Environment
AsyncMac - Remote Access Mac
atapi - atapi
Beep - Beep
CardS - CardS
Cdrom - Cdrom
Disk - Disk
DPIFLTNT - DPIFLTNT
DTA - DTA
E190x - 3Com 3C90x Adapter Driver
Enabler - Enabler
intlfxsr - intlfxsr
Kbdclass - Keyboard Class Driver
KSecDD - KSecDD
L8042prt - Logitech Keyboard and PS/2 Mouse Port Driver
lkbdfltr - Logitech Keyboard Class Filter Driver
lmoufltr - Logitech Mouse Class Filter Driver
ltmodem - Actiontec 56K V.90 Modem Driver
maestro - maestro
Mouclass - Mouse Class Driver
Msfs - Msfs
NDIS - Microsoft NDIS System Driver
NdisTapi - Microsoft NDIS TAPI driver
NdisWan - Remote Access WAN Wrapper
-- More --

Note: The ICE template that you will design in this exercise searches the output of the ntodrv command for any lines that contain the word "modem," such as the line highlighted in Figure 1-8.

Building the modem ICE template

The ICE template determines which command or script is to be run, where that command resides, and what the ICE module should do with the output of the command. In this exercise you will use the Template Editor to create four template records: OS/Release, Base Path, Script Entry, and Message Maps. At the end of this exercise, your ICE template should look like Figure 1-9.

Figure 1-9 ICE template for NTODrv exercise



To create an ICE template based on NTODrv

To create an ICE template based on netstat, first create a new ICE template and then create the following four template records:

- OS/Release
- Base Path
- Script Entry
- Message Maps

To create an ICE template

1. In the Symantec ESM console tree, right-click **Templates** and select **New**.
2. Select **Integrated Command Engine - all** from the list of available template types.
3. Name the new template **modem**.

   Note: Do not name the template with a .ice file extension. Symantec ESM automatically adds the .ice extension.

4. Click **OK** and Symantec ESM automatically launches the Template Editor.

To add the OS/Release record to your modem ICE template

1. In the Template Editor, click **Add Row** to create a new template record.
2. Click the cell under the Name column to access the Name drop-down list and select **OS/Release**.
3. Delete all <NEW> entries from fields.
4. Click the **OS/Rev** button to launch the OS/Rev Sublist Editor. The button displays the number of entries in the OS/Rev sublist. Initially the number is set to 0.
5. In the OS/Rev Sublist Editor, click **Add Row** to add a new sublist record.
6. Click the cell under the OS column to access the OS drop-down list and select the operating system where you want to run the netstat command.

   Note: To run the program on agents installed on different Windows versions, you can create a second sublist record for Windows 2000 or Windows NT.

7. Uncheck the Exclude check box.
8. Delete the <NEW> entry in the Release/Revision column.
9. Click **Apply** and then **Close** to return to the Template Editor.

To add the Base Path record to your netstat ICE template

1. In the Template Editor, click **Add Row**.
2. Select **Base Path** from the Name drop-down list.
3. Remove all <NEW> entries from fields.
4. Type **scripts** in the Script ID -or- Base Path column on the Base Path template record. See row 2 in Figure 1-9.

   The Base Path tells the ICE module where the command program is located within the ESM directory. Using installation defaults, **scripts** points to c:\Program Files\Symantec\Esm\Scripts on Windows systems.

To add the Script Entry record to your netstat ICE template

1. In the Template Editor, click **Add Row**.
2. Select **Script Entry** from the Name drop-down list.
3. Delete all <NEW> entries from fields.
4. Type **NTODrv command** in the Script ID -or- Base Path column of the Script Entry template record.
5. Type **ntodrv.exe** in the Script Name column of the Script Entry template record. This is the name of the program that the ICE module will execute. Your entries will match row 3 in Figure 1-9 on page 16. No Script Parameters are needed with the ntodrv command

To add the Message Maps record to your netstat ICE template

1. In the Template Editor, click **Add Row**.
2. Select **Message Maps** from the Name drop-down list.
3. Delete all <NEW> entries from fields.
4. Click the **Message Maps** button to launch the Message Maps Sublist Editor. The button displays the number of entries in the OS/Rev sublist. Initially the number is set to 0.

Note: You must define at least one message map so the ICE module will know what to do with the output of the netstat command. You can map the command output to any of the ICE module messages. See Table 1-2, "ICE module messages," on page 10.

---

5. In the Message Maps Sublist Editor, click **Add Row**.
6. Click the cell under the Message column and select **User #1/4** from the drop-down list. This is a red level, user-customized message.
7. In the Map String field, replace the <NEW> entry by typing **modem**.

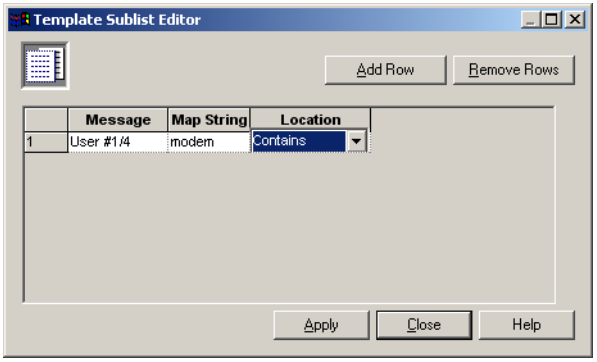
Note: Message Maps sublist entries are case sensitive.

---

8 Click the cell under the Location column and select **Contains** from the drop-down list. This instructs the ICE module to capture all ntodrv data that contains the text "modem."

Your message map sublist record should look like Figure 1-10.

Figure 1-10 Message map sublist record



9 Click **Apply** and **Close** to close the Template Sublist Editor.

10 Click **Save** and **Close** to save your netstat.ice template.

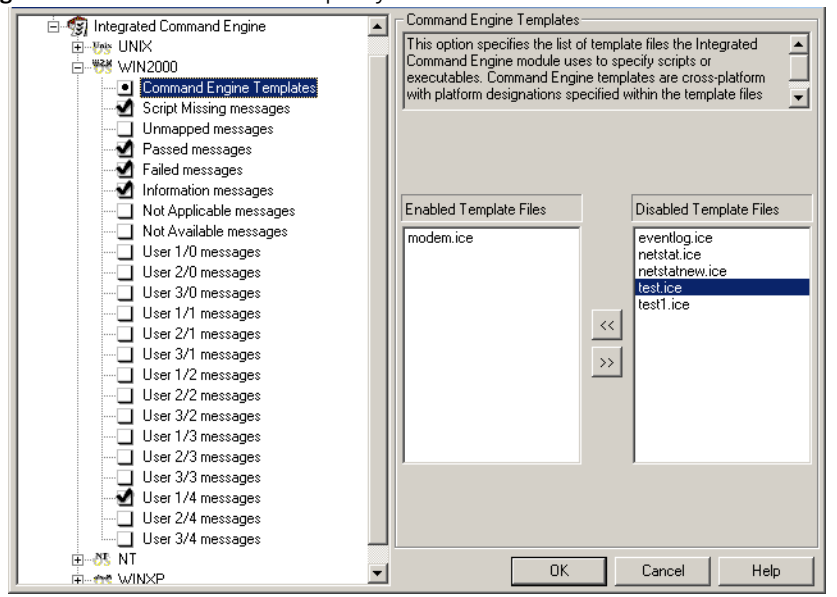
Running the ICE module and modem.ice template

You can now run the ICE module to execute the ntodrv command and capture its output, using the modem.ice template you have created.

To run the ICE module and capture NTODrv output

1. Create a new Symantec ESM demonstration policy and add the ICE module to it. For information on creating and using policies, see your *Symantec ESM User Manual*.
2. Open the new policy and enable your modem.ice template by selecting the **Command Engine Templates** option and moving the modem.ice template to the Enabled Template Files name list.
3. Verify that the messages that you expect the ICE module to produce are enabled in the ICE module. Your policy should look like Figure 1-11. Click **OK** to close your demonstration policy.

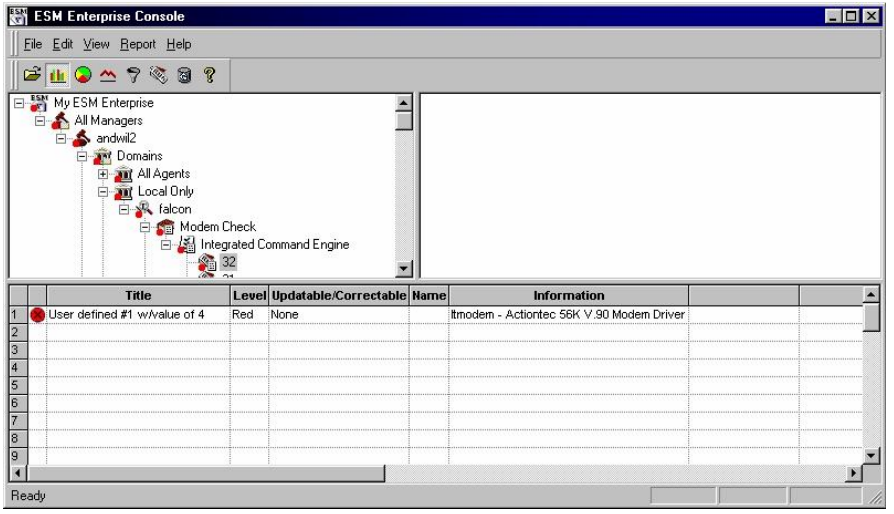
Figure 1-11 Modem check policy



4 Run the demonstration policy on the Windows system where you installed the NTOdrv utility. This should take only a few moments depending on the speed of the system and the latency in the network.

After the policy has run, the report data should look something like Figure 1-12.

Figure 1-12 Modem check policy run report



Additional NTODrv exercises

Test what you have learned in the preceding sections of this guide by completing the following additional exercises.

Exercise 1

Enhance the modem.ice template to make allowances for case variations (e.g. Modem, MODEM).

Exercise 2

Search for additional drivers that may or may not be desired and map appropriate messages to those occurrences.

PSLogList exercise

This exercise shows you how to integrate the PSLogList utility into the ICE module. In this exercise you will:

- Run the PSLogList utility with the -s parameter to display the contents of the Windows Event Log on a Windows NT, Windows 2000, or Windows XP system and review the output.
- Define the Event Log data that you want to capture in an ICE template.
- Run the ICE module to capture and report Event Log data.
- Complete related training exercises to test what you have learned.

Running PSLogList and reviewing its output

PSLogList is a utility that displays the contents of the Event Log from a local or remote computer. Viewing the contents of the Event Log lets you monitor certain types of event notifications that occur in a customer's environment.

Using PSLogList with the ICE module is not meant as a substitute for real-time event monitoring. Real-time event monitoring is best accomplished using a tool such as Symantec Intruder Alert or Symantec Host IDS.

Download the PSLogList utility from http://www.sysinternals.com

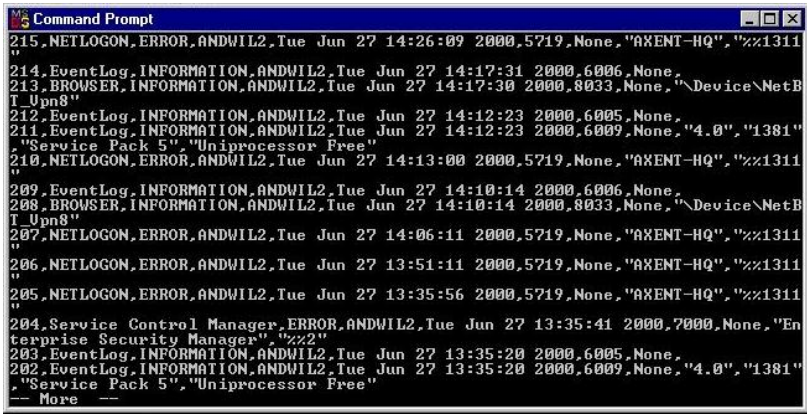
---

Note: PSLogList is also bundled with several command line administration tools and can be downloaded as PSTools.

To run PSLogList and review its output

1. If it doesn't already exist, create the Scripts subdirectory in the ESM directory (usually c:\Program Files\Symantec\ESM on Windows) on at least one of the Symantec ESM manager/agent systems that will be used for this training exercise.
2. Copy psloglist.exe to the Scripts directory.
3. Run the psloglist command with the -s parameter and watch the output, which should look like this:

Figure 1-13 PSLogList output

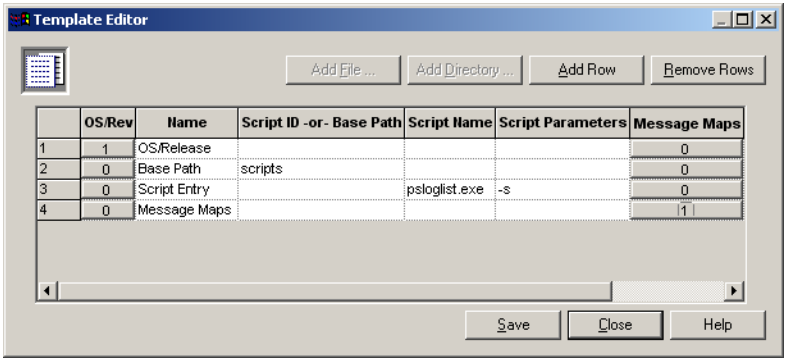


Note: The ICE template that you will design in this exercise searches for NetLogon "ERROR" messages that indicate domain logon failures. This illustrates how information can be extracted from the Event Log. In a production environment, you would build the template to report service failures.

Building the eventlog ICE template

The ICE template determines which command or script is to be run, where that command resides, and what the ICE module should do with the output of the command. In this exercise you will use the Template Editor to create four template records: OS/Release, Base Path, Script Entry, and Message Maps. At the end of this exercise, your ICE template should look like Figure 1-14.

Figure 1-14 ICE Template for PSLogList exercise



To create an ICE template based on PSLogList

To create an ICE template based on netstat, first create a new ICE template and then create the following four template records:

- OS/Release
- Base Path
- Script Entry
- Message Maps

To create an ICE template

1. In the Symantec ESM console tree, right-click **Templates** and select **New**.
2. Select **Integrated Command Engine - all** from the list of available template types.
3. Name the new template **eventlog**.

   Note: Do not name the template with a .ice file extension. Symantec ESM automatically adds the .ice extension.

4. Click **OK** and Symantec ESM automatically launches the Template Editor.

To add the OS/Release record to your modem ICE template

1. In the Template Editor, click **Add Row** to create a new template record.
2. Click the cell under the Name column to access the Name drop-down list and select **OS/Release**.
3. Delete all <NEW> entries from fields.
4. Click the **OS/Rev** button to launch the OS/Rev Sublist Editor. The button displays the number of entries in the OS/Rev sublist. Initially the number is set to 0.
5. In the OS/Rev Sublist Editor, click **Add Row** to add a new sublist record.
6. Click the cell under the OS column to access the OS drop-down list and select the operating system where you want to run the netstat command.

   Note: To run the program on agents installed on different Windows versions, you can create a second or third sublist record for Windows XP, Windows 2000, or Windows NT.

7. Uncheck the Exclude check box.
8. Delete the <NEW> entry in the Release/Revision column.
9. Click **Apply** and then **Close** to return to the Template Editor.

To add the Base Path record to your netstat ICE template

1. In the Template Editor, click **Add Row**.
2. Select **Base Path** from the Name drop-down list.
3. Remove all <NEW> entries from fields.
4. Type **scripts** in the Script ID -or- Base Path column on the Base Path template record. See row 2 in Figure 1-14.

   The Base Path tells the ICE module where the command program is located within the ESM directory. Using installation defaults, **scripts** points to \Program Files\Symantec\Esm\Scripts on Windows systems.

To add the Script Entry record to your netstat ICE template

1. In the Template Editor, click **Add Row**.
2. Select **Script Entry** from the Name drop-down list.
3. Delete all <NEW> entries from fields.
4. Type **psloglist command** in the Script ID -or- Base Path column of the Script Entry template record.
5. Type **psloglist.exe** in the Script Name column of the Script Entry template record. This is the name of the program that the ICE module will execute.
6. Type -s in the Script Parameters field to tell the ICE module to run psloglist command with the -s parameter. Your entries will match row 3 in Figure 1-14 on page 24.

To add the Message Maps record to your netstat ICE template

1. In the Template Editor, click **Add Row**.
2. Select **Message Maps** from the Name drop-down list.
3. Delete all <NEW> entries from fields.
4. Click the **Message Maps** button to launch the Message Maps Sublist Editor. The button displays the number of entries in the OS/Rev sublist. Initially the number is set to 0.

   Note: You must define at least one message map so the ICE module will know what to do with the output of the netstat command. You can map the command output to any of the ICE module messages. See Table 1-2, "ICE module messages," on page 10.

   ---

5. In the Message Maps Sublist Editor, click **Add Row**.

6 Click the cell under the Message column and select **Informational** from the drop-down list. This is a green level message that is intended to report information output from a command.

7 In the Map String field, replace the <NEW> entry by typing **NETLOGON,ERROR**.

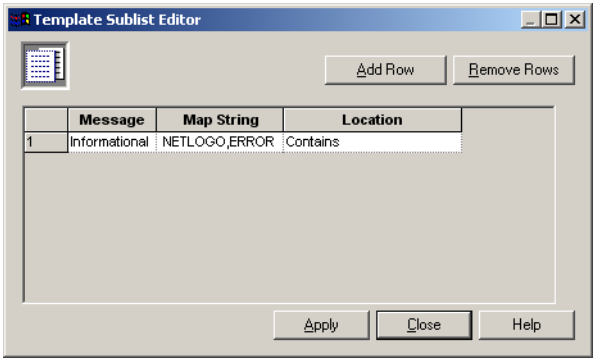
Note: Message Maps sublist entries are case sensitive.

---

8 Click the cell under the Location column and select **Contains** from the drop-down list. This instructs the ICE module to capture all Event Log data that contains the text "NETLOGON,ERROR."

Your message map sublist record should look like Figure 1-15.

Figure 1-15 Message map sublist record



9 Click **Apply** and **Close** to close the Template Sublist Editor.

10 Click **Save** and **Close** to save your netstat.ice template.

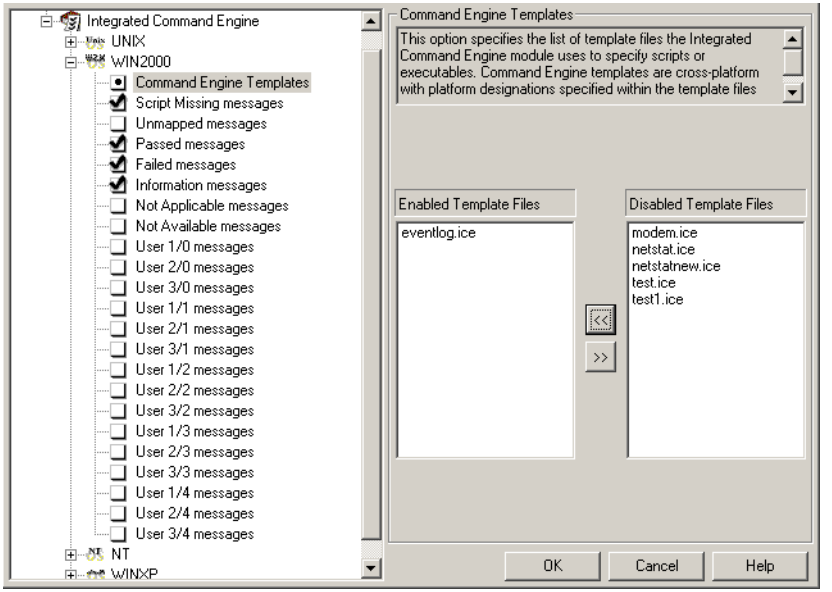
Running the ICE module and eventlog.ice template

You can now run the ICE module to execute the psloglist command and capture its output, using the eventlog.ice template that you have created.

To run the ICE module and capture PSLogList output

1. Create a new Symantec ESM demonstration policy and add the ICE module to it. For information on creating and using policies, see your *Symantec ESM User Manual*.
2. Open the new policy and enable your eventlog.ice template by selecting the **Command Engine Templates** option and moving the eventlog.ice template to the Enabled Template Files name list.
3. Verify that the messages that you expect the ICE module to produce are enabled in the ICE module. Your policy should look like Figure 1-16. Click **OK** to close your demonstration policy.

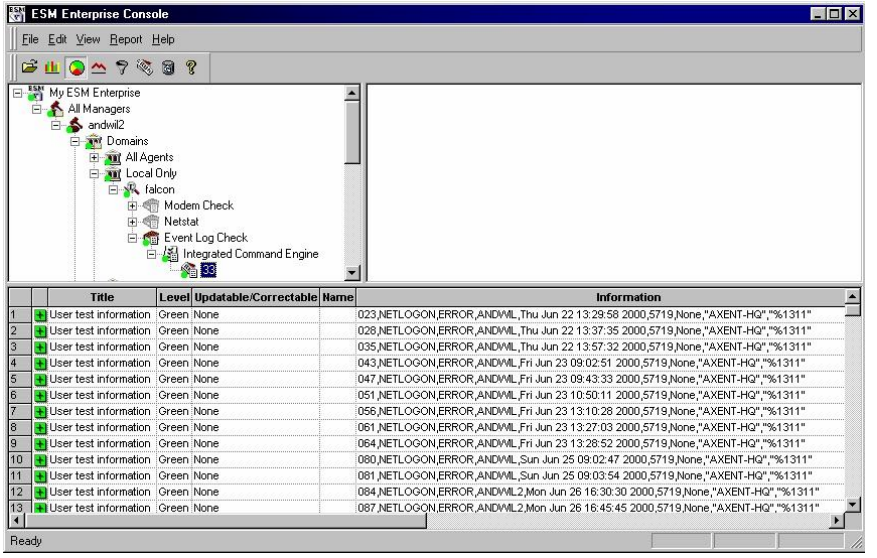
Figure 1-16 Event Log check policy



4 Run the demonstration policy on the Windows system where you installed the PSLogList utility. This should take only a few moments, depending on the speed of the system and the latency in the network.

After the policy has run, the report data should look something like Figure 1-17.

Figure 1-17 Event log check policy run report


ESM Enterprise Console
File Edit View Report Help
My ESM Enterprise
All Managers
andwil2
Domains
All Agents
Local Only
falcon
Modem Check
Netstat
Event Log Check
Integrated Command Engine
Title Level Updatable/Correctable Name Information
1 User test information Green None 023,NETLOGON,ERROR,ANDWIL,Thu Jun 22 13:29:58 2000,5719,None,"AXENT-HQ","%1311"
2 User test information Green None 028,NETLOGON,ERROR,ANDWIL,Thu Jun 22 13:37:35 2000,5719,None,"AXENT-HQ","%1311"
3 User test information Green None 035,NETLOGON,ERROR,ANDWIL,Thu Jun 22 13:57:32 2000,5719,None,"AXENT-HQ","%1311"
4 User test information Green None 043,NETLOGON,ERROR,ANDWIL,Fri Jun 23 09:02:51 2000,5719,None,"AXENT-HQ","%1311"
5 User test information Green None 047,NETLOGON,ERROR,ANDWIL,Fri Jun 23 09:43:33 2000,5719,None,"AXENT-HQ","%1311"
6 User test information Green None 051,NETLOGON,ERROR,ANDWIL,Fri Jun 23 10:50:11 2000,5719,None,"AXENT-HQ","%1311"
7 User test information Green None 056,NETLOGON,ERROR,ANDWIL,Fri Jun 23 13:10:28 2000,5719,None,"AXENT-HQ","%1311"
8 User test information Green None 061,NETLOGON,ERROR,ANDWIL,Fri Jun 23 13:27:03 2000,5719,None,"AXENT-HQ","%1311"
9 User test information Green None 064,NETLOGON,ERROR,ANDWIL,Fri Jun 23 13:28:52 2000,5719,None,"AXENT-HQ","%1311"
10 User test information Green None 080,NETLOGON,ERROR,ANDWIL,Sun Jun 25 09:02:47 2000,5719,None,"AXENT-HQ","%1311"
11 User test information Green None 081,NETLOGON,ERROR,ANDWIL,Sun Jun 25 09:03:54 2000,5719,None,"AXENT-HQ","%1311"
12 User test information Green None 084,NETLOGON,ERROR,ANDWIL2,Mon Jun 26 16:30:30 2000,5719,None,"AXENT-HQ","%1311"
13 User test information Green None 087,NETLOGON,ERROR,ANDWIL2,Mon Jun 26 16:45:45 2000,5719,None,"AXENT-HQ","%1311"
Ready

Additional PSLogList exercise

Test what you have learned in the preceding sections of this guide by completing the following additional exercise.

Exercise 1

Enhance the eventlog.ice template to report service failures.